PKF F.R.A.N.T.S
Chartered Accountants
DHA, Phase IV, Karachi
Other Offices in Islamabad| Lahore | Peshawar| Multan| Sialkot| Kabul

+92 (21) 3531 5274-76
Karachi@pkf.com.pk
www.pkf.com.pk

Dated: **23rd October 2024**

The Chief Regulatory Officer
Pakistan Stock Exchange Limited
2nd Floor, Administration Block,
Stock Exchange Road,
Karachi.

Dear Sir,

SUB: AGREED-UPON PROCEDURES FOR REVIEW & TESTING OF CATALYST IT SOLUTIONS (PVT.) LIMITED ORDER MANAGEMENT SYSTEM (OMS) & BACK-OFFICE SYSTEM, APPLICATION SOURCE CODE REVIEW AND VAPT

We are pleased to enclose herewith one copy of the Audit Report as per PSX Minimum Information Security Standards.

Thanking You,

Yours Truly,

PKF F.R.A.N.T.S.

Chartered Accountants
Place: Karachi

PKF F.R.A.N.T.S
Chartered Accountants
DHA, Phase IV, Karachi
Other Offices in Islamabad| Lahore | Peshawar| Multan| Sialkot| Kabul

+92 (21) 3531 5274-76
Karachi@pkf.com.pk
www.pkf.com.pk

Methodology:

The IT audit will be conducted using a structured approach to evaluate the compliance of Securities Brokers with the Minimum Information Security Standards prescribed by the Pakistan Stock Exchange (PSX). The methodology will include the following steps:

1. **Planning and Scoping**:
   - Define the scope of the audit, focusing on the key areas outlined in the PSX standards such as access controls, data security, network security, and vendor management.
   - Identify the relevant software, applications, and processes used by the Securities Brokers for trading, risk management, clearing, and settlement.
2. **Data Collection**:
   - Gather necessary documents such as security policies, incident logs, system architecture diagrams, and audit trails to assess the implementation of controls.
   - Conduct interviews with IT personnel, management, and other stakeholders to understand the procedures and security measures in place.
   - Utilize technical tools and scripts to collect data related to access management, encryption practices, and system configurations.
3. **Compliance Assessment**:
   - Review the broker's compliance with the PSX guidelines on critical areas like authentication, password policies, multi-factor authentication, and user access management.
   - Verify the implementation of encryption for sensitive data at rest and in transit, and evaluate the measures in place to protect data confidentiality.
4. **Technical Testing**:
   - Perform vulnerability assessments and penetration testing (if applicable) on key systems to identify potential security risks.
   - Test remote connectivity, firewalls, and intrusion detection systems to ensure they provide adequate protection against unauthorized access.
   - Review physical and environmental controls to verify the protection of critical IT infrastructure.
5. **Gap Analysis**:
   - Identify any gaps between the current practices of the broker and the PSX-prescribed standards.
6. **Reporting**:
   - Prepare a comprehensive audit report that includes the findings of the compliance assessment, technical testing results, and identified risks.
   - Provide actionable recommendations to address deficiencies, strengthen security controls, and ensure compliance with PSX standards.

This methodology ensures a thorough evaluation of the IT security posture of the Securities Brokers, aligning with both regulatory requirements and industry best practices.

Audit Report
CATALYST IT SOLUTIONS OMS (Order Management System) & BackOffice System
As per PSX Minimum Information Security standards

Objectives:

The goal of this audit report is to ensure that the Securities brokers adhere to the minimal statistics safety requirements set by way of the Pakistan stock exchange (PSX). This consists of comparing compliance with mounted hints for software program, packages, and protection controls, assessing risk control practices, and making sure the confidentiality, integrity, and availability of vital statistics and structures. The audit pursuits to perceive vulnerabilities, confirm the adequacy of carried out controls, and recommend improvements for mitigating potential cyber security threats, thereby safeguarding capital marketplace operations.

Executive Summary:

CATALYST IT Solutions Order management System (OMS) & Backoffice System including all their components were audited to ensure compliance with the Minimum Information Security Standards as prescribed by the Pakistan Stock Exchange (PSX). The audit focused on key areas such as Access Controls, Data Security, Password Management, Business Continuity and Disaster Recovery, and Incident Management. This report provides findings, highlights areas of compliance, and identifies areas for improvement in the system.

1. Purpose and Scope:

The purpose of this audit is to evaluate the Order management System's adherence to the Minimum Information Security Standards prescribed by the Pakistan Stock Exchange (PSX). The audit focuses on key compliance areas such as access controls, data security, network and communications security, password management, patch management, incident management, and business continuity. The scope includes assessing the effectiveness of the system's security controls, identifying potential vulnerabilities, and ensuring the system’s capability to protect sensitive data, comply with regulatory requirements, and mitigate risks associated with cyber security threats.

2. Key areas of compliance:

2.1 ***Access Controls***

- **PSX requirement:**
  - User access must be controlled through unique user IDs, passwords, and multi-factor authentication for all critical systems.
  - Strict role-based access must be implemented, ensuring users are granted access on a need-to-know basis.
  - Inactive sessions must be locked or terminated after a period of inactivity, and access should be reviewed annually.
  - Administrative privileges should be assigned separately from regular user IDs, and logs must be maintained for all access and administrative activities
- **OMS:**

  The Order management system adheres to robust access control policies:

  - The system employs a unique user ID such as the username for all accounts.
  - Log-on information is only validated upon complete input; ensuring error conditions do not reveal which part of the input is correct or incorrect.
  - User accounts are locked after five failed login attempts, enhancing security against brute-force attacks.
  - Idle sessions timeout after a period of inactivity, preventing unauthorized access. Both unattended and normal modes in the application are covered under this policy.
  - MFA is implemented at login to add an additional layer of security
  - Users are required to change their password upon first login to prevent unauthorized access.
  - A user rights and role matrix is in place for the segregation of duties, ensuring that roles are clearly defined, and access is granted on a need-to-know basis.
  - Accounts become dormant after 90 days of inactivity.

- **Audit Findings:**
  - Fully compliant with PSX standards for access control.

2.2 Password Management:

- **PSX requirement:**
  - Passwords must be at least 8 characters long.
  - Must include at least three of the following: uppercase letters, lowercase letters, numbers, and special characters.
  - Passwords should expire every 30 days.
  - Reuse of the last 3 passwords is not allowed.
  - Users must change the password upon first login.
  - Passwords must not be stored in clear text; they should be encrypted.

- Accounts should lock after 5 failed login attempts.
- A detailed log report of password activities should be maintained.

- **OMS:**
  The system's password management follows best practices:
  - Passwords expire every 30 days, forcing users to regularly update their credentials.
  - Passwords require a minimum length of 8 characters and must include a mix of uppercase letters, lowercase letters, numbers, and special characters.
  - The system prevents users from reusing their last three passwords, enhancing password security.
  - Passwords are not stored in clear text; they are encrypted on storage devices, ensuring that even system administrators do not have access to plain text passwords.
  - A user log report is generated, capturing the date, time, IP address, and user activities for accountability and audit purposes.

- **Audit Findings:**
  - The password management policies are in full compliance with PSX security standards.

2.3 User Administration:

- **PSX requirement:**
  - User creation and modifications must follow a maker-checker process to prevent unauthorized changes.
  - Detailed logs must be maintained for every action performed by administrators.
  - There must be a dedicated module for managing user accounts.
  - The system should generate reports such as User Access Summary, User Access Details, and Administrator Actions.
  - No single individual should be able to make changes to access rights without proper authorization.

- **OMS:**
  - The system generates detailed logs for all administrative activities.
  - A separate module for managing users exists, fulfilling PSX requirements.
  - The required reports (User Access Summary, User Access Details, and Information Security Administrator Reports) are available in the system.
  - OMS implements role-based segregation, ensuring proper distribution of access control duties.

- **Audit Findings:**
  - User administration policies are compliance with PSX standard but users are not following the maker checker process.

- **Recommendation:**
  - User creation must be followed by maker and checker concept.

- **Remedial Procedure:**
  - **Action**
    - The system does not allow the creation of a user with a single user.
  - **Timeline**
    - 30 to 50 working days.

2.4 Data Security

- **PSX requirement:**
  - Critical data must be encrypted at all times, both at rest and in transit.
  - Strict access controls should be applied to limit personnel access to sensitive data, with logs and audits for administrative activities.
  - Backup data must be regularly maintained and secured, and a clear data retention and disposal policy must be implemented

- **OMS:**
  - Critical data is both stored and transmitted in an encrypted format, ensuring the protection of sensitive information.
  - The system regularly performs data backups, although the frequency of backups was not detailed.
  - Users without the appropriate permissions cannot print or export sensitive data, safeguarding information from unauthorized dissemination.

- **Audit Findings:**
  - Compliant with PSX standards for data security.

2.5 Network and Communications Security

- **PSX requirement:**
  - Ensure that network infrastructure is protected through firewalls, intrusion detection/prevention systems (IDS/IPS), and appropriate encryption mechanisms.
  - Segregate internal and external networks to limit exposure, and ensure data transmission over public or wireless networks is encrypted using secure protocols like TLS.
  - Ensure regular reviews of network architecture and apply adequate measures against malware and virus attacks.
- **OMS:**
  - All data transmitted over the network is encrypted, reducing the risk of interception or breaches during data transit.
  - Remote access to critical systems is restricted, monitored, and logged; ensuring that only authorized personnel can access the system from external networks.

- **Audit Findings**
  - The system meets the requirements for network and communication security, ensuring compliance with PSX standards

2.6 Patch Management

- **PSX requirement**
  - Establish a patch management process that prioritizes and implements security updates in a timely manner.
  - Perform testing before deployment to prevent unintended system impacts and ensure all patches are applied following a documented change management process.
  - Automatic patching features should be enabled where feasible to keep systems secure.
- **OMS**
  - Regular application vulnerability assessments, code reviews, and code testing are conducted to ensure the system remains secure and up-to-date.
  - The process for applying patches is thorough, but the audit did not find documentation on the specific timelines for patch implementation.

- **Audit Findings**
  - Clearly define patch timelines for different levels of vulnerabilities (e.g., critical, medium, low) to ensure timely updates.
  - fully compliant with PSX standards

2.7 Incident Management

- **PSX requirement:**
  - Establish written policies for reporting, managing, and escalating information security incidents.
  - Maintain a central log of incidents, accessible to authorized personnel, and ensure that all employees are aware of their responsibility to report any incidents.

- **OMS:**
  - Security incidents are logged and reported, allowing for tracking and follow-up on any breaches or vulnerabilities.
  - There is no incident response plan in place for addressing security breaches.

- **Audit Findings:**
  - Conduct regular drills to validate the effectiveness of the incident response.
  - Partially Compliant with PSX incident management standards, but there is a need to establish the policies.
- **Recommendation:**
  - Proper Polices define for incident management and security breach.
  - Proper training provided to users for incident handling.

- **Remedial Procedure:**
  - **Action**
    - Incident management policies making and user training.
  - **Timeline**
    - 60 to 70 working days.

2.8 Physical and Environmental Security

- **PSX requirement:**
  - Implement security perimeters to protect critical IT infrastructure, and restrict physical access to authorized personnel only.
  - Monitor physical access through CCTV or other controls, and ensure data centers are protected from physical threats such as power failure or environmental risks.
  - Secure removable media and ensure secure disposal of hardware containing sensitive data

- **OMS:**
  - Physical access to critical systems is restricted and monitored; ensuring only authorized individuals can enter secure areas.
  - Adequate environmental controls, such as fire prevention and power backup systems, were not covered in detail.

- **Audit Findings:**
  - Compliant, though further details on environmental controls are advised.

2.9 Business Continuity and Disaster Recovery

- **PSX requirement:**
  - A comprehensive Business Continuity Plan (BCP) and Disaster Recovery (DR) plan must be in place to ensure operational integrity in case of incidents.
  - BCP/DR plans must be regularly tested and reviewed annually to ensure alignment with business needs, and employees should be trained to implement these plans.
  - The plans must cover critical business processes and services provided by third parties, with documented agreements and backup measures
- **OMS:**
  - There is a disaster recovery plan in place, with clearly defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), established with business consent.
  - Regular drills are conducted to validate the business continuity plan, ensuring that the system can recover effectively from potential disruptions.

- **Audit Findings:**
  - Ensure drills are performed frequently, with reports generated and reviewed to improve response times.
  - Fully compliant with PSX business continuity and DR standards.

3. Compliance Summary:

Here is a table summarizing the key compliance areas based on the PSX standards and the OMS audit results:

Category	PSX Requirement	OMS Compliance	Audit Recommendation
Access Controls	Unique user ID, password management, MFA, session timeout	Compliant	Access Controls measures are complied
Password Management	Minimum 8 characters, password expiry, no clear-text storage	Compliant	System Comply with Password Management Standard.
User administration	Detailed report, detailed module, checking process, detailed logs, segregation of duties	Partially Compliant	Maker and Checker must be enforcing while creating user.
Data Security	Data encryption (at rest and in transit), data backup	Compliant	System Comply with Data Security Standards.
Network and Communications Security	Encryption of transmitted data, network segregation, firewall	Compliant	Encrypted communication, monitored remote access
Patch Management	Regular patching, documented timeline for critical updates	Compliant	Regular vulnerability assessments and patch management follows.
Incident Management	Incident response plan, logging, reporting breaches	Partially Compliant	Incident Reporting policies must be defined and training session provided to users.
Physical and Environmental Security	Restricted physical access, environmental controls	Compliant	Compliant, though further details on environmental controls are advised.
Business Continuity and Disaster Recovery	BCP/DR plan, regular drills, RTO, RPO	Compliant	System complies with Business continuity and Disaster recovery

4. Management Response:

We acknowledge the audit findings related to two (2) of our partial compliance with PSX incident management standards and the recommendation to formalize policies for incident management and security breaches.

In response, we have already begun implementing corrective actions. Within the next two months, we will initiate a comprehensive training program for clients on incident handling and management. This program will ensure that all users are well-versed in incident response procedures and adhere to the newly established policies, enhancing the overall security framework.

Additionally, regarding the audit finding on user administration policies, we recognize the need for stricter enforcement of the maker-checker process, despite our current compliance with PSX standards. While the maker-checker functionality was previously available, clients were permitted to bypass this feature. To enhance security and eliminate this vulnerability, we will implement a system update in our upcoming December release. After this update, user creation will strictly follow the maker-checker protocol, ensuring compliance with the required security standards.

These steps demonstrate our commitment to addressing the audit recommendations and strengthening our processes to meet industry standards effectively.

5. Conclusion:

The CATALYST OMS & Backoffice offers secure operational functionality that largely adheres to PSX Minimum Information Security Standards. However, there are areas for improvement, such as user administration, employee training and incident management policies. By addressing these shortcomings, they can significantly strengthen the OMS system's security and operational efficiency.

Action Items:

- User creation must be followed by maker and checker concept.
- Employee Awareness and training session on security and incident reporting.

PKF F.R.A.N.T.S.

Chartered Accountants
Place: Karachi